



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001184789 A**(43) Date of publication of application: **06.07.01**

(51) Int. Cl.

G11B 20/10
G06F 12/14
G09C 5/00
H04L 9/32

(21) Application number: **11366074**(22) Date of filing: **24.12.99**(71) Applicant: **TAIYO YUDEN CO LTD**

(72) Inventor: **OMURA YUKIHIRO**
SUNAKAWA RYUICHI

(54) **OPTICAL INFORMATION RECORDING MEDIUM,
 METHOD AND SYSTEM FOR HOLDING
 INFORMATION SECRECY**

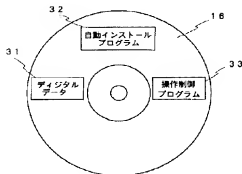
the inputted password is a regular password,
 interrupted operation is continued.

COPYRIGHT: (C)2001,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an optical information recording medium, a method and a system for holding information secrecy, with which the illegal use or the like of recorded information can be prevented.

SOLUTION: When recording information on a CD-R 16, in addition to digital data 31, an automatic install program 32 and an operation control program 33 are written together. When the CD-R 16 is loaded into an information reproducing device, the automatic install program 32 is automatically started and the operation control program is made resident and started in the memory of the information reproducing device. When operation to digital data written on the CD-R 16 is detected, the operation control program 33 calls the entry of a password by interrupting this operation and when



(51) Int. Cl. ⁷	機別記号	F I	テマコード(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 D 0 4 4
G 0 9 C 5/00		G 0 9 C 5/00	5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 9 A 0 0 1
			6 7 3 C
審査請求 未請求 請求項の数21 O L (全 14 頁)			

(21) 出願番号 特願平11-366074

(22) 出願日 平成11年12月24日(1999. 12. 24)

(71) 出願人 000204284

太陽誘電株式会社
東京都台東区上野6丁目16番20号

(72) 発明者 大村 幸秀

東京都台東区上野6丁目16番20号 太陽誘
電株式会社内

(72) 発明者 砂川 隆一

東京都台東区上野6丁目16番20号 太陽誘
電株式会社内

(74) 代理人 100069981

弁理士 吉田 結孝 (外1名)

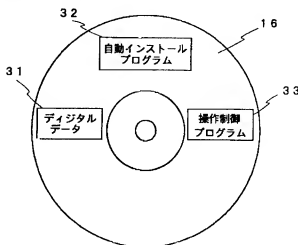
最終頁に続く

(54) 【発明の名称】 光情報記録媒体並びに情報機密保持方法及びそのシステム

(57) 【要約】

【課題】 記録情報の不正使用等を防止できる光情報記録媒体並びに情報機密保持方法及びそのシステムを提供する。

【解決手段】 情報をCD-R 16に記録する際に、デジタルデータ31に加えて、自動インストールプログラム32と操作制御プログラム33と一緒に書き込む。自動インストールプログラム32は、CD-R 16を情報再生装置へ装填したときに自動的に起動して操作制御プログラムを情報再生装置のメモリに常駐起動させ、操作制御プログラム33はCD-R 16内に書き込まれているデジタルデータへの操作を検出したときに、この操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに中断していた操作を継続させる処理を行う。



【特許請求の範囲】

【請求項1】 デジタルデータと、

前記デジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第1のコンピュータプログラムと、

少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置への装填時に、自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムとを記録されていることを特徴とする光情報記録媒体。

【請求項2】 前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれたデジタルデータであることを特徴とする請求項1記載の光情報記録媒体。

【請求項3】 前記デジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したデジタルデータであることを特徴とする請求項1記載の光情報記録媒体。

【請求項4】 前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれたデジタルデータであり、

前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいることを特徴とする請求項1記載の光情報記録媒体。

【請求項5】 前記デジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したデジタルデータであり、

前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいることを特徴とする請求項1記載の光情報記録媒体。

【請求項6】 前記第1のコンピュータプログラムは、検出対象とする前記デジタルデータへの操作の1つとして、前記デジタルデータの複写操作を含んでいることを特徴とする請求項1記載の光情報記録媒体。

【請求項7】 追記型の光情報記録媒体であることを特徴とする請求項1記載の光情報記録媒体。

【請求項8】 前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれ且つ該電子透かしデータの一部分に前記正規のパスワードが含まれているデジタルデータであり、

前記第1のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワード

とを比較する手段とを含んでいることを特徴とする請求項1記載の光情報記録媒体。

【請求項9】 光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用するときの情報機密保持方法であって、

前記光情報記録媒体に対して前記情報を書き込むときに、

前記情報に基づくデジタルデータと、

該デジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第1のコンピュータプログラムと、

前記情報再生装置への装填時に、自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムとを前記光情報記録媒体に書き込むことを特徴とする情報機密保持方法。

【請求項10】 前記光情報記録媒体に対して前記情報を書き込むときに、

前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだ前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとすることを特徴とする請求項9記載の情報機密保持方法。

【請求項11】 前記光情報記録媒体に対して前記情報を書き込むときに、

前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成した後、さらに該データを暗号化して前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとすることを特徴とする請求項9記載の情報機密保持方法。

【請求項12】 前記第1のコンピュータプログラムを、検出対象とする前記デジタルデータへの操作の1つとして前記デジタルデータの複写操作を含んだものとすることを特徴とする請求項9記載の情報機密保持方法。

【請求項13】 前記光情報記録媒体として追記型の光情報記録媒体を用いることを特徴とする請求項9記載の情報機密保持方法。

【請求項14】 前記光情報記録媒体に対して前記情報

を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものとすることを特徴とする請求項9記載の情報機密保持方法。

【請求項15】 情報記録装置を用いて光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用する情報機密保持システムであって、前記情報記録装置は、機密保持対象となるデジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第1のコンピュータプログラムを保持する手段と、前記情報再生装置への装填時に自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムを保持する手段と、

前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくデジタルデータと共に前記第1のコンピュータプログラムと前記第2のコンピュータプログラムとを前記光情報記録媒体に書き込む手段を備えていることを特徴とする情報機密保持システム。

【請求項16】 前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、

前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記デジタルデータを生成する手段を備えていることを特徴とする請求項15記載の情報機密保持システム。

【請求項17】 前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、

前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、該電子透かしデータが埋め込まれたデータを暗号化して前

記デジタルデータを生成する手段とを備えていることを特徴とする請求項15記載の情報機密保持システム。

【請求項18】 前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号する外部プログラムを動作させて復号されたデジタルデータを得る手段と、該復号されたデジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段とを含んだものであり、

前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、該電子透かしデータが埋め込まれたデータを暗号化して前記デジタルデータを生成する手段とを備え、前記情報再生装置は、前記暗号化されたデジタルデータを復号するコンピュータプログラムを前記外部プログラムとして備えていることを特徴とする請求項15記載の情報機密保持システム。

【請求項19】 前記第1のコンピュータプログラムは、検出対象とする前記デジタルデータへの操作の1つとして前記デジタルデータの複写操作を含んだものであることを特徴とする請求項15記載の情報機密保持システム。

【請求項20】 前記光情報記録媒体が追記型の光情報記録媒体であることを特徴とする請求項15記載の情報機密保持システム。

【請求項21】 前記第1のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものであり、

前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記デジタルデータを生成する手段を備えていることを特徴とする請求項15記載の情報機密保持システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報機密保持能力を向上させた光情報記録媒体及び情報機密保持方法及びそのシステムに関するものである。

【0002】

【従来の技術】近年、パーソナルコンピュータやオーディオ・ビジュアル機器を含む各種の電子機器発達が目覚ましく、高性能で低価格のこの種の商品が普及するようになった。これに伴い、パーソナルコンピュータやオーディオ・ビジュアル機器に使用されるデジタルデータ

も多種に亘り、デジタルデータ等のソフト商品の販売や流通も盛んになっている。

【0003】一方、事務処理等もコンピュータを用いて行うことがほとんどであり、扱うデジタルデータの量も膨大な量となっている。このため、万に備えてCD-Rなどの情報記録媒体にデータのバックアップを取っておくことも一般的に行われている。

【0004】このような状況下において、コンピュータを扱える人の数は急増し、デジタルデータのコピーも容易に行えることから、オリジナルのデジタルデータをコピーした複製を不正に作成して、それを他人に再配布したり、或いは機密保持を有する情報が漏洩してしまう可能性がある。

【0005】これらの不正使用を防止するために、データの暗号化技術や一般的に電子透かしと呼ばれる技術が研究されている。

【0006】データの暗号化とは、主としてコンピュータネットワークにおいて複数の人物がデータをやりとりする時に、データそのものを守るために開発されてきた技術で、悪意のある第三者がデータを取得して使用したり或いは改ざんしたりすることを防止するために用いられている。

【0007】この暗号化技術を用いると、暗号化されたデータはこのデータをやりとりする人間にしか解読できないようになり、第三者がデータを取得してもその内容を解読することはできない。

【0008】この暗号化技術としては、暗号化データを復号するときにデータを暗号化したときの暗号鍵を共通に用いる共通鍵方式と、暗号化するための鍵を公開鍵として他者に対して公開しておき、復号化のための鍵を個人鍵として自分自身の手に保管しておく公開鍵方式が、一般的に広く用いられている。

【0009】電子透かしとは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する情報を、デジタルデータ自体に埋め込む技術である。この技術を応用することによって、例えば、不正コピーが発見された場合に、誰がその不正コピーを再配布したのかを特定することも可能である。また、電子透かしの技術を実現する方法としては、現在、離散コサイン変換、フーリエ変換、ウェーブレット変換等を用いた方法が研究されている。

【0010】

【発明が解決しようとする課題】しかしながら、暗号化技術や電子透かし技術を用いて加工したデジタルデータであっても、他の情報記録媒体に不正にコピーすることは可能である。これを防止するためには、情報記録媒体への情報記録装置或いは情報再生装置又は双方の機能を備えた情報記録再生装置に不正コピーを防止するための特殊な機能を設ける必要があるが、未だ実現に至っていない。

【0011】本発明の目的は上記の問題点に鑑み、記録情報の不正使用等を防止できる光情報記録媒体並びに情報機密保持方法及びそのシステムを提供することである。

【0012】

【課題を解決するための手段】本発明は上記の目的を達成するために請求項1では、デジタルデータと、前記デジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第1のコンピュータプログラムと、少なくともメモリに常駐するコンピュータプログラムとを動作させる情報再生装置への装填時に、自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムとが記録されている光情報記録媒体を提案する。

【0013】該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第2のコンピュータプログラムが起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第1のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記デジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記デジタルデータのコピー操作、前記デジタルデータが文字情報や画像情報である場合はその表示操作、前記デジタルデータがコンピュータプログラムである場合にはその実行操作、前記デジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第1のコンピュータプログラムは、前記情報再生装置から前記デジタルデータへの操作を検出したときに、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のデジタルデータを操作することができない。

【0014】また、請求項2では、請求項1記載の光情報記録媒体において、前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれたデジタルデータである光情報記録媒体を提案する。

【0015】該光情報記録媒体では、前記デジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータである。これにより、正規パスワードを入力して前記デジタルデータを操作しても、操作後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。

【0016】また、請求項3では、請求項1記載の光情報記録媒体において、前記デジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したデジタルデータである光情報記録媒体を提案する。

【0017】該光情報記録媒体では、前記デジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータである。これにより、正規パスワードを入力して前記デジタルデータを操作しても、前記デジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。

【0018】また、請求項4では、請求項1記載の光情報記録媒体において、前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれたデジタルデータであり、前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいる光情報記録媒体を提案する。

【0019】該光情報記録媒体では、前記デジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータである。これにより、正規パスワードを入力して前記デジタルデータを操作しても、操作後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0020】また、請求項5では、請求項1記載の光情報記録媒体において、前記デジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したデジタルデータであり、前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいる光情報記録媒体を提案する。

【0021】該光情報記録媒体では、前記デジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータである。これにより、正規パスワードを入力して前記デジタルデータを操作しても、前記デジタルデータを

復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0022】また、請求項6では、請求項1記載の光情報記録媒体において、前記第1のコンピュータプログラムは、検出対象とする前記デジタルデータへの操作の1つとして、前記デジタルデータの複写操作を含んでいる光情報記録媒体を提案する。

【0023】該光情報記録媒体では、前記正規のパスワードを入力しなければ前記デジタルデータを複写、即ちコピーすることができない。

【0024】また、請求項7では、請求項1記載の光情報記録媒体において、追記型の光情報記録媒体である光情報記録媒体を提案する。

【0025】該光情報記録媒体は追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【0026】また、請求項8では、請求項1記載の光情報記録媒体において、前記デジタルデータは、基本データに対して電子透かしデータが埋め込まれ且つ該電子透かしデータの一部分に前記正規のパスワードが含まれているデジタルデータであり、前記第1のコンピュータプログラムは、前記電子透かしデータを前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んでいる光情報記録媒体を提案する。

【0027】該光情報記録媒体では、前記電子透かしデータ内に前記正規のパスワードが含まれているため、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【0028】また、請求項9では、光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用するときの情報機密保持方法であって、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくデジタルデータと、該デジタルデータへの操作を検出したときに該操作を中断させるパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときにコンピュータ中断した操作を継続させる処理を行う第1のコンピュータプログラムと、前記情報再生装置への装着時に、自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムとを前記光情報記録媒体に書き込む情報機密保持方法を提案する。

【0029】該情報機密保持方法によれば、光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくデジタルデータと、前記第1及び第2のコンピュータプログラムが書き込まれるので、該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第2のコンピュータプログラムが起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第1のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記デジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記デジタルデータのコピー操作、前記デジタルデータが文字情報や画像情報である場合はその表示操作、前記デジタルデータがコンピュータプログラムである場合にはその実行操作、前記デジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第1のコンピュータプログラムは、前記情報再生装置から前記デジタルデータへの操作を検出したとき、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のデジタルデータを操作することができない。

【0030】また、請求項10では、請求項9記載の情報機密保持方法において、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとする情報機密保持方法を提案する。

【0031】該情報機密保持方法によれば、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータが前記デジタルデータとして光情報記録媒体に書き込まれる。これにより、正規パスワードを入力して前記デジタルデータを操作しても、操作後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0032】また、請求項11では、請求項9記載の情報機密保持方法において、前記光情報記録媒体に対して

前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成した後、さらに該データを暗号化して前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとする情報機密保持方法を提案する。

【0033】該情報機密保持方法によれば、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記デジタルデータとして光情報記録媒体に書き込まれる。これにより、正規パスワードを入力して前記デジタルデータを操作しても、前記デジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0034】また、請求項12では、請求項9記載の情報機密保持方法において、前記第1のコンピュータプログラムを、検出対象とする前記デジタルデータへの操作の1つとして前記デジタルデータの復号操作を含んだものとする情報機密保持方法を提案する。

【0035】該情報機密保持方法によれば、前記正規のパスワードを入力しなければ前記デジタルデータを複写即ちコピーすることができない。

【0036】また、請求項13では、請求項9記載の情報機密保持方法において、前記光情報記録媒体として追記型的光情報記録媒体を用いる情報機密保持方法を提案する。

【0037】該情報機密保持方法によれば、前記光情報記録媒体が追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【0038】また、請求項14では、請求項9記載の情報機密保持方法において、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記デジタルデータを生成し、前記第1のコンピュータプログラムを、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものとする情報機密保持方法を提案する。

【0039】該情報機密保持方法によれば、前記電子透かしデータ内に前記正規のパスワードが含まれているた

め、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【0040】また、請求項15では、情報記録装置を用いて光情報記録媒体に情報を書き込み、少なくともメモリに常駐させるコンピュータプログラムを動作させる情報再生装置を用いて前記情報を書き込まれている光情報記録媒体から前記情報を取り出して利用する情報機密保持システムであって、前記情報記録装置は、機密保持対象となるデジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第1のコンピュータプログラムを保持する手段と、前記情報再生装置への装填時に自動的に起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第2のコンピュータプログラムを保持する手段と、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくデジタルデータと共に前記第1のコンピュータプログラムと前記第2のコンピュータプログラムとを前記光情報記録媒体に書き込む手段を備えている情報機密保持システムを提案する。

【0041】該情報機密保持システムによれば、前記情報記録装置によって光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくデジタルデータと、前記第1及び第2のコンピュータプログラムが書き込まれるので、該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第2のコンピュータプログラムが起動して前記第1のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第1のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記デジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記デジタルデータのコピー操作、前記デジタルデータが文字情報や画像情報である場合はその表示操作、前記デジタルデータがコンピュータプログラムである場合にはその実行操作、前記デジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第1のコンピュータプログラムは、前記情報再生装置から前記デジタルデータへの操作を検出したときに、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のデジタルデータを操作することができない。

【0042】また、請求項16では、請求項15記載の情報機密保持システムにおいて、前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記

基本データの読み出し操作であるときに、前記デジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記デジタルデータを生成する手段を備えている情報機密保持システムを提案する。

【0043】該情報機密保持システムによれば、前記情報記録装置によって書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータが前記デジタルデータとして光情報記録媒体に書き込まれる。これにより、情報再生装置において正規パスワードを入力して前記デジタルデータを操作しても、操作後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0044】また、請求項17では、請求項15記載の情報機密保持システムにおいて、前記第1のコンピュータプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、該電子透かしデータが埋め込まれたデータを暗号化して前記デジタルデータを生成する手段とを備えている情報機密保持システムを提案する。

【0045】該情報機密保持システムによれば、前記情報記録装置において書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記デジタルデータとして光情報記録媒体に書き込まれる。これにより、前記情報再生装置において正規パスワードを入力して前記デジタルデータを操作しても、前記デジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0046】また、請求項18では、請求項15記載の情報機密保持システムにおいて、前記第1のコンピュ

タブプログラムは、前記デジタルデータへの操作が前記基本データの読み出し操作であるときに、前記デジタルデータを復号する外部プログラムを動作させて復号されたデジタルデータを得る手段と、該復号されたデジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段とを含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、該電子透かしデータが埋め込まれたデータを暗号化して前記デジタルデータを生成する手段とを備え、前記情報再生装置は、前記暗号化されたデジタルデータを復号するコンピュータプログラムを前記外部プログラムとして備えている情報機密保持システムを提案する。

【0047】該情報機密保持システムによれば、前記情報記録装置において書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記デジタルデータとして光情報記録媒体に書き込まれる。これにより、前記情報再生装置において正規パスワードを入力して前記デジタルデータを操作しても、前記デジタルデータを復号できなければ前記基本情報を得ることはできない。また、前記情報再生装置に前記暗号化されたデジタルデータを復号するコンピュータプログラムが存在しなければ、前記暗号化されたデジタルデータを復号することはできない。さらに、前記暗号化データを復号できても、復号後のデジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記デジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【0048】また、外部プログラムが、CD-ROM、CD-R等でデータと共に配信される場合は、バージョンアップの際に互換性を考慮する必要が低くなる。また、CD-ROM上の外部プログラムをOS (Operating System) レベルで起動させるようにすれば、外部プログラムのコピーを困難にすることも可能である。

【0049】また、請求項19では、請求項15記載の情報機密保持システムにおいて、前記第1のコンピュータプログラムは、検出対象とする前記デジタルデータへの操作の1つとして前記デジタルデータの複写操作を含んだものである情報機密保持システムを提案する。

【0050】該情報機密保持システムによれば、前記正規のパスワードを入力しなければ前記デジタルデータを複写即ちコピーすることができない。

【0051】また、請求項20では、請求項15記載の情報機密保持システムにおいて、前記光情報記録媒体が

追記型の光情報記録媒体である情報機密保持システムを提案する。

【0052】該情報機密保持システムによれば、前記光情報記録媒体が追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【0053】また、請求項21では、請求項15記載の情報機密保持システムにおいて、前記第1のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記デジタルデータを生成する手段を備えている情報機密保持システムを提案する。

【0054】該情報機密保持システムによれば、前記電子透かしデータ内に前記正規のパスワードが含まれており、前記第1のコンピュータプログラムは該正規のパスワードを抽出して比較に用いているため、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【0055】

【発明の実施の形態】以下、図面に基づいて本発明の実施形態を説明する。

【0056】図1は、本発明の第1の実施形態における情報機密保持システムを示す外観図、図2はその電気系回路示すブロック図である。図において、1は情報機密保持システムで、パーソナルコンピュータ本体11、モニター12、キーボード13、マウス14、CD-Rライター15及び一般的にCD-Rと称されているライトワンス追記型光ディスク（以下、CD-Rと称する）16から構成されている。

【0057】パーソナルコンピュータ本体（以下、コンピュータ本体と称する）11は、周知のCPU21、メモリ22、表示制御部23、ハードディスク装置24、フロッピーディスク装置25、及びCDドライブ装置26を備えている。

【0058】CPU21には、表示制御部23を介してモニター12が接続されると共に、図示せぬインタフェースを介してキーボード13、マウス14及びCD-Rライター15が接続されている。

【0059】CPU21は、ハードディスク装置24に格納されているプログラムをメモリ22内に読み込み或いはメモリに常駐させ、このメモリ22内のプログラムによって動作する。また、CPU21は、表示制御部23を介してモニター12に情報の表示を行うと共に、キーボード13及びマウス14を介して入力されたデータ及び命令を読み込むと共にこれを実行する。さらに、C

PU21は、ハードディスク装置24内のデータをアクセスすると共に、フロッピーディスク装置25及びCDドライブ装置に装填されたフロッピーディスクまたはCD内のデータをアクセスする。

【0060】ハードディスク装置24には、各種のアプリケーションプログラムやデータが格納され、本願発明に係るアプリケーションプログラムとして、電子透かし埋め込みモジュール、CD-R記録モジュール、自動インストールプログラム、操作制御プログラム及び機密情報書き込みモジュールが格納されている。

【0061】次に、上記のシステムを用いてCD-R16に機密情報を記録する際の操作及びCPU21の動作を説明する。

【0062】CD-R16に機密情報を記録するときは、前述した機密情報書き込みモジュールを起動する。起動後、CPU21はこのモジュールのプログラムに従って図3に示す通り動作して情報の記録処理を行う。

【0063】即ち、機密情報書き込みモジュールを起動すると、CPU21は、まずパスワードの設定画面を表示してパスワードの設定を促す(SA1)。このパスワードは操作者が任意に設定するもので、記録した情報を操作する際に使用するものである。

【0064】次いで、CPU21は、記録対象となる情報のファイルの指定を促し、操作者によってファイルが指定されると、電子透かし埋め込みモジュールを起動して指定されたファイルのデジタルデータ(基本データ)に対して電子透かしデータを埋め込んだデジタルデータを生産する(SA2)。このとき、電子透かしデータの一部に、前記SA1の処理で設定されたパスワードが正規パスワードとして埋め込まれる。また、パスワード以外の電子透かしデータは、電子透かし埋め込みモジュールを起動することによって任意に設定可能になっている。

【0065】この後、CPU21は、CD-R記録モジュールを起動して、CD-Rライター15に装填されているCD-R16に対して、上記電子透かしが埋め込まれたデジタルデータと共に自動インストールプログラム及び操作制御プログラムをCD-R16に書き込む。これにより、図4に示すように、電子透かしが埋め込まれたデジタルデータ31、自動インストールプログラム32及び操作制御プログラム33が記録されたCD-R16が作成され、機密情報の記録処理が終了する。

【0066】上記処理によって情報が記録されたCD-R16内のデジタルデータ31は、上記の正規パスワードを知っている者だけが操作できるようになり、パスワードを知らない者は一切の操作を行うことができない。

【0067】即ち、自動インストールプログラムは、これが書き込まれているCD-R16が情報再生装置のCDドライブ装置に装填されると自動的に起動して、操作

制御プログラムを情報再生装置のメモリに常駐させて動作させる機能をする。

【0068】従って、CD-R16を情報再生装置のCDドライブ装置に装填すると操作制御プログラムによる操作規制制御が行われる。

【0069】例えば、コンピュータ本体11のCDドライブ装置26に上記の機密情報を記録したCD-R16を装填すると、自動インストールプログラム32が自動的に起動して、操作制御プログラム33をメモリ22に常駐させて起動させる。

【0070】操作制御プログラムが情報再生装置のメモリ内で動作を開始すると、CPU21は、CDドライブ装置に装填されたCDに書き込まれているデジタルデータに対する情報記録再生装置からの操作を監視し、電子透かしデータが埋め込まれたデータに対する操作を規制する。

【0071】この操作は、例えばデジタルデータのコピー操作、デジタルデータが文字情報や画像情報である場合はその表示操作、デジタルデータがコンピュータプログラムである場合にはその実行操作、デジタルデータが音声情報である場合はその再生操作等である。

【0072】即ち、図5に示すように、CPU21は、CD-R16内のデジタルデータ31に対する操作を監視(SB1、SB2)、このデジタルデータ31に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する(SB3)。

【0073】次いで、CPU21は、デジタルデータ31から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する(SB4)。

【0074】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて(SB5)、後述するSB7の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、CPU21は、上記中断していた操作を実行する(SB6)。

【0075】次に、CPU21は、CDドライブ装置26からCD-R16が取り出された否かを判定し(SB7)、取り出されていないときは上記SB1の処理に移行して前述の処理を繰り返し、CDドライブ装置26からCD-R16が取り出されたときは、上記の処理を終了して操作制御プログラム33をメモリ22から開放する。

【0076】従って、CD-R16に書き込まれているデジタルデータ31は、パスワードを知っている者だけが操作することができる。パスワードを知らない者は、データのコピー、データの表示、プログラムの実行、データの音声再生等を行うことができない。これにより、CD-R16に書き込まれているデジタルデータ31の不正使用や改竄を防止することができる。

【0077】尚、本実施形態では、正規パスワードを電子透かしデータの一部としてデジタルデータ31に埋め込むようにしたが、操作制御プログラム33内に埋め込むようにしても良い。また、これら双方を用いて異なる2つのパスワードをそれぞれに埋め込んで2重に規制するようにしても良い。

【0078】次に、本発明の第2の実施形態を説明する。

【0079】第2の実施形態では、第1の実施形態の構成に加えて、他のアプリケーションプログラムからCD-R16内のデジタルデータ16を読み出して使用する場合には、デジタルデータ31から電子透かしデータを除去してからアプリケーションプログラムに引き渡す機能を、操作制御プログラム33に設けた。

【0080】即ち、コンピュータ本体11のCDドライブ装置26に上記の機密情報を記録したCD-R16が装填されて操作制御プログラム33が起動されると、図6に示すように、CPU21は、CD-R16内のデジタルデータ31に対する操作を監視し(SC1、SC2)、このデジタルデータ31に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する(SC3)。

【0081】次いで、CPU21は、デジタルデータ31から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する(SC4)。

【0082】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて(SC5)、後述するSC11の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、CPU21は、他のアプリケーションプログラムからのデータ読み出し操作であるか否かを判定する(SC6)。

【0083】この判定の結果、他のアプリケーションプログラムからのデータ読み出し操作でないときは、上記中断していた操作を実行して(SC7)、後述するSC11の処理に移行する。また、他のアプリケーションプログラムからのデータ読み出し操作であるときは、CD-R16からデジタルデータ31を読み出されて(SC8)、デジタルデータ31から電子透かしデータを除去したデジタルデータを生成し(SC9)、このデジタルデータを上記アプリケーションプログラムに引き渡す(SC10)。

【0084】次に、CPU21は、CDドライブ装置26からCD-R16が取り出された否かを判定し(SC11)、取り出されていないときは上記SC11の処理に移行して前述の処理を繰り返し、CDドライブ装置26からCD-R16が取り出されたときは、上記の処理を終了して操作制御プログラム33をメモリ22から開放する。

【0085】これにより、上記他のアプリケーションプログラムは、デジタルデータ31を電子透かしデータを除去した状態で使用することができる。従って、例えば目に見える電子透かしを用いた画像データを表示する場合にも、自動的に電子透かしが除去され、電子透かしのない画像データを表示させることができる。

【0086】次に、本発明の第3の実施形態を説明する。

【0087】第3の実施形態は、第2の実施形態の構成に加えて、CD-R16へのデータ書き込みの際にデジタルデータ31を暗号化するようにした。このための暗号モジュールはハードディスク装置24に格納されている。

【0088】第3の実施形態では、CD-R16に機密情報を記録するために機密情報書き込みモジュールを起動すると、図7に示すように、CPU21は、まずパスワードの設定画面を表示してパスワードの設定を促す(SD1)。このパスワードは、前述と同様に操作者が任意に設定するもので、記録した情報を操作する際に使用するものである。

【0089】次いで、CPU21は、記録対象となる情報のファイルの指定を促し、操作者によってファイルが指定されると、電子透かし埋め込みモジュールを起動して指定されたファイルのデジタルデータ(基本データ)に対して電子透かしデータを埋め込んだデジタルデータを生成する(SD2)。さらに、CPU21は、操作制御プログラム内に、前記SD1の処理で設定されたパスワードを正規パスワードとして埋め込んだ操作制御プログラム33を生成する。

【0090】この後、CPU21は、暗号モジュールを起動して、上記電子透かしデータが埋め込まれたデジタルデータを暗号化したデジタルデータを生成して(SD3)、デジタルデータ31とする。

【0091】次に、CD-R記録モジュールを起動して、CD-Rライター15に装填されているCD-R16に対して、上記電子透かしが埋め込まれたさらに暗号化されたデジタルデータ31と共に自動インストールプログラム32及び正規パスワードを埋め込んだ操作制御プログラム33をCD-R16に書き込む。

【0092】これにより、機密情報の記録処理が終了する。

【0093】一方、情報再生装置のCDドライブ装置に、例えばコンピュータ本体11のCDドライブ装置26に、上記の機密情報を記録したCD-R16が装填されて操作制御プログラム33が起動すると、CPU21は次のように動作してデジタルデータ31に対する操作規制を行う。

【0094】即ち、図8に示すように、CPU21は、CD-R16内のデジタルデータ31に対する操作を監視し(SE1、SE2)、このデジタルデータ31

に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する(SE3)。

【0095】次いで、CPU21は、デジタルデータ31から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する(SE4)。

【0096】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて(SE5)、後述するSC11の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、CPU21は、他のアプリケーションプログラムからのデータ読み出し操作であるか否かを判定する(SE6)。

【0097】この判定の結果、他のアプリケーションプログラムからのデータ読み出し操作でないときは、上記中断していた操作を実行して(SE7)、後述するSE12の処理に移行する。また、他のアプリケーションプログラムからのデータ読み出し操作であるときは、CD-R16からデジタルデータ31を読み出して(SE8)、暗号モジュールを起動して復号を行う(SE9)。

【0098】この復号処理においては、鍵(共通鍵或いは公開鍵)を必要とするため、鍵を持たない者は復号できない。

【0099】次いで、CPU21は、復号が終了した暗号モジュールを開放し、復号したデジタルデータ31から電子透かしデータを除去したデジタルデータを生じ(SEL10)、このデジタルデータを上記アプリケーションプログラムに引き渡す(SEL11)。

【0100】次に、CPU21は、CDドライブ装置26からCD-R16が取り出されたか否かを判定し(SEL12)、取り出されていないときは上記SEL1の処理に移行して前述の処理を繰り返す。CDドライブ装置26からCD-R16が取り出されたときは、上記の処理を終了して操作制御プログラム33をメモリ22から開放する。

【0101】このようにデータを暗号化することにより、機密保持機能をさらに向上させることができる。

【0102】尚、上記第1乃至第3の実施形態は、本発明の一具体例であって、本発明がこれらのみに限定されることはない。

【0103】また、上記各実施形態では、機密情報をCD-R16に書き込んで保存する場合に関して述べたが、これに限定されることはなく、第3者の不正使用を避けたい情報等であれば、同様に実施でき同様の効果が得られる。

【0104】また、上記各実施形態では、情報記録媒体としてCD-R16を用いたがこれに限定されることはない。しかし、ライトワンス追記型のCD-Rを用いることによりデータの改竄防止効果は大きくなる。

【0105】また、上記各実施形態では、電子透かしデータを埋め込んだデジタルデータへの操作規制制御を行ったが、操作制御プログラムによって、電子透かしデータを埋め込んでいないデジタルデータを含めて、CD-R16に書き込まれた全てのデータ及びプログラムに対して操作規制するようにしても良い。

【0106】また、上記各実施形態では、情報の書き込みを行った情報機密保持システム1を用いて、情報が書き込まれたCD-R16に対するデータ操作を行った例を説明したが、他の情報再生装置等を用いても同様の効果が得られることが言うまでもないことである。

【0107】

【発明の効果】以上説明したように本発明の請求項1乃至請求項8記載の光情報記録媒体によれば、パスワードを知らない者は、書き込まれているデジタルデータへの操作を行うことができないので、前記デジタルデータの不正使用や改竄を防止することができる。

【0108】また、請求項9乃至請求項14記載の情報機密保持方法によれば、該方法によって情報が書き込まれた光情報記録媒体内の情報を操作するときに、パスワードを知らない者は、書き込まれているデジタルデータへの操作を行うことができないので、前記デジタルデータの不正使用や改竄を防止することができる。

【0109】また、請求項15乃至請求項21記載の情報機密保持システムによれば、該システムの情報記録装置を用いて情報が書き込まれた光情報記録媒体内の情報を操作するときに、パスワードを知らない者は、書き込まれているデジタルデータへの操作を行うことができないので、前記デジタルデータの不正使用や改竄を防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態における情報機密保持システムを示す外觀図

【図2】本発明の第1の実施形態における情報機密保持システムの電気系回路示すブロック図

【図3】本発明の第1の実施形態における機密情報書き込み処理を説明するフローチャート

【図4】本発明の第1の実施形態における機密情報が書き込まれたCD-Rを示す概念図

【図5】本発明の第1の実施形態における操作制御動作を説明するフローチャート

【図6】本発明の第2の実施形態における操作制御動作を説明するフローチャート

【図7】本発明の第3の実施形態における機密情報書き込み処理を説明するフローチャート

【図8】本発明の第3の実施形態における操作制御動作を説明するフローチャート

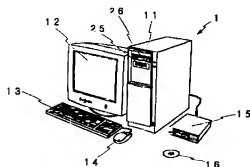
【符号の説明】

1…情報機密保持システム、11…パーソナルコンピュータ本体、12…モニター、13…キーボード、14…

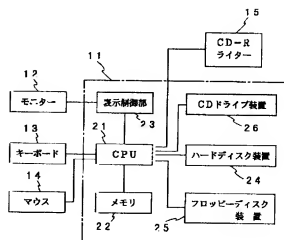
マウス、15…CD-Rライター、16…CD-R、21…CPU、22…メモリ、23…表示制御部、24…ハードディスク装置、25…フロッピーディスク装置、

26…CDドライブ装置、31…デジタルデータ、32…自動インストールプログラム、33…操作制御プログラム。

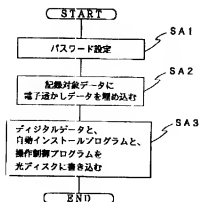
【図1】



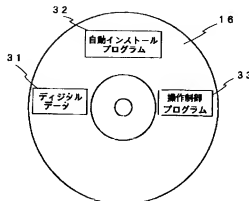
【図2】



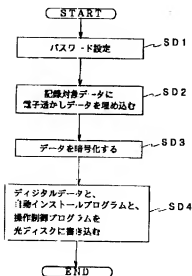
【図3】



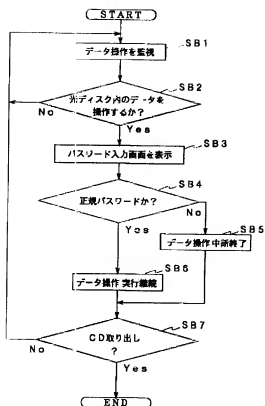
【図4】



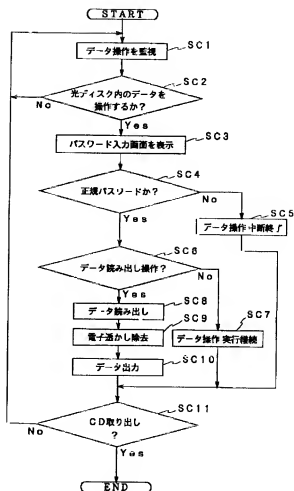
【図7】



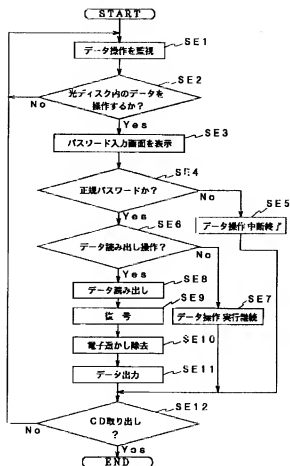
【図5】



【図6】



【図8】



フロントページの続き

Fターム(参考) 5B017 AA06 BA05 BA07 BB02 CA09

CA16

5D044 BC05 CC04 DE47 DE49 DE57

GK12 GK17

5J104 AA01 AA07 AA14 KA01 NA05

NA32 PA14

9A001 EE03 LL03